UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,629	08/16/2001	Steven Dale Goodman	RPS9 2001 0046	2708

45211 7590 05/26/2006

KELLY K. KORDZIK
WINSTEAD SECHREST & MINICK PC
PO BOX 50784
DALLAS, TX 75201

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/26/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/931,629
Filing Date: August 16, 2001
Appellant(s): GOODMAN ET AL.

Toni L. Stanley
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8 May 2006 appealing from the Office action mailed 20 September 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Alexander et al. U.S Patent No. 6,188,602

Grawrock U.S Patent No. 6,678,833

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1 – 4 and 6 –10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alexander (U.S. Patent 6,188,602), in view of Grawrock (U.S. Patent 6,678,833).

With regards to claim 1, Alexander teaches a method for updating a program in a data processing system comprising the steps of:

modifying the program with the update to the program in response to the unlocking of the memory unit storing the program (Alexander: Column 5 Line 46 – 52, Column 5 Line 41 – 45 and Column 5 Line 60 – 61).

Alexander fails to teach the use of a trusted platform module ("TPM") to perform a signature verification of an update to the program.

Grawrock teaches:

requesting a trusted platform module ("TPM") to perform a signature verification of an update to the program; and the TPM performing the signature verification of the update to the program (Grawrock: Column 4 Line 1 – 18; Alexander: Column 5 Line 41 – 45, Column 5 Line 60 – 62 and Figure 3A / state Element 340 directed to state Element 342: Examiner notes First of all, the Alexander reference is relied upon validating the BIOS data prior to loading the new BIOS update image. Besides, the reliance of the signature verification performed at TPM on the BIOS image is laid upon the Grawrock reference (Grawrock: Column 4 Line 1 – 18));

if the signature verification of the update to the program is successful, unlocking a memory unit storing the program (Alexander, Column 5 Line 58 – 62 and Column 5 Line 32 – 45; Grawrock, Column 4 Line 1 – 18).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock's TPM within the system of Alexander's memory device because it offers the advantages of allowing the TPM to accurately report the identity of the boot block without reliance on any intervening devices (Grawrock: Column 2 Line 1 – 6).

With regards to claim 2, 6 and 9, Alexander teaches locking the memory unit after the modifying step (Alexander: Column 5 Line 62 – 64).

With regards to claim 3, Alexander teaches the locking step is performed by the TPM (Alexander: Column 5 Line 62 – 64, Grawrock: Column 4 Line 1 – 9).

With regards to claim 4, Alexander teaches a computer program product adaptable for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprising:

a BIOS update application program receiving an updated BIOS image (Alexander: Column 5 Line 1 – 13);

the BIOS update application modifies the BIOS with the updated BIOS image (Alexander: Column 5 Line 41 – 45);

Alexander fails to teach the use of TPM to perform a signature verification of an update to the program.

Grawrock teaches:

the BIOS update application requesting a TPM to perform a signature verification of the updated BIOS image (Grawrock: Column 4 Line 1 – 18; Alexander: Column 5 Line 46 – 52);

a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image (Grawrock: Column 4 Line 1 – 18; Alexander: Column 5 Line 30 – 67); and

the TPM program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to the BIOS update application (Grawrock: Column 4 Line 1 – 9; Alexander: Column 5 Line 30 – 67);

if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash

memory (Alexander: Column 5 Line 58 – 62, Grawrock: Column 4 Line 1 – 9; Alexander: Column 5 Line 30 – 67).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock's TPM within the system of Alexander's memory device because it offers the advantages of allowing the TPM to accurately report the identity of the boot block without reliance on any intervening devices (Grawrock: Column 2 Line 1 – 6).

With regards to claim 7 and 10, Alexander teaches if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic, then an error message is output (Grawrock: Column 5 Line 34 – 38; Alexander: Column 5 Line 36 – 40).

With regards to claim 8, Alexander teaches a data processing system having circuitry for updating a BIOS stored in a flash memory in the data processing system, comprising:

circuitry for modifying the BIOS with the updated BIOS image (Alexander: Column 5 Line 41 – 45).

Alexander fails to teach the use of TPM to perform a signature verification of an update to the program.

Grawrock teaches:

input circuitry for receiving an updated BIOS image (Grawrock: Figure 3 & Column 3 Line 50 – 56; Alexander: Column 5 Line 30 – 67);

circuitry for requesting a TPM to perform a signature verification of the updated BIOS image (Grawrock: Figure 3 & Column 4 Line 10 – 18; Alexander: Column 5 Line 30 – 67);

the TPM performing the signature verification of the updated BIOS image (Grawrock: Figure 3 & Column 3 Line 1 – 19; Alexander: Column 5 Line 30 – 67);

the TPM unlocking the flash memory if the signature verification of the updated BIOS image determines that the updated BIOS image is authentic (Alexander: Column 5 Line 58 – 62; Grawrock: Column 4 Line 1 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock's TPM within the system of Alexander's memory device because it offers the advantages of allowing the TPM to accurately report the identity of the boot block without reliance on any intervening devices (Grawrock: Column 2 Line 1 – 6).

(10) Response to Argument

In the instant appeal brief, Applicant has the presented the following arguments:

1. On page 5 (4th Para), Applicant has alleged that the Alexander and Grawrock references teach (a) flashed memory is unlocked before the program is updated, and (b) the program is installed and updated first and

thereafter verify the program and Applicant asserts this is opposed of what is recited in the claim.

2. On page 5 (3rd Para), Applicant has alleged that in state 330, the flash memory is reset to a read/write access, as taught by Alexander, is the same as unlocking the flash memory and thereby Applicant asserts Alexander teaches the flashed memory is unlocked before the program is updated as opposed of what is recited in the claim (Appeal Brief, Page 5, 3rd – 4th Para).

1. Alexander teaches flashed memory is locked before the program is updated.

On page 5 (4th Para), Applicant has alleged that the Alexander and Grawrock references teach (a) flashed memory is unlocked before the program is updated, and (b) the program is installed and updated first and thereafter verify the program and Applicant asserts this is opposed of what is recited in the claim. Examiner respectfully disagrees. In view of Alexander reference, Examiner asserts the program update cycle into the flash memory starts with the runtime mode (i.e. Alexander: Figure 3A Element 304) when flash memory is in locked state, which is distinct from Applicant's assertion that the program update cycle starts at the power-on reset state (i.e. Alexander: Figure 3A Element 302). The purpose of power-on reset state is to access the flash memory in order to get the computer started. In state 330,

the flash memory is reset to a read/write access, as taught by Alexander, to unlock the flash memory – this is for the purpose of reading the BIOS at start-up which is similar to Applicant's Declaration filed on Oct. 24, 2005 (under 37 C.F.R. §1.132). However, the program update cycle in practice starts from computer runtime mode when the flash memory is locked. For the purpose of clarity, the complete cycle for each of the program update into the flash memory, as taught by Alexander, is presented as follows – (1) when each of the update is complete, the system passes control from RBU (Remote BIOS Update) state to power on reset state and reset all blocks in flash memory to "locked" status, and then pass control to run state (Alexander: Column 5 Line 13 – 17) – i.e. the flash memory is normally protected in "locked" status after program update; (2) when a system management program requests an update of information in flash memory, the system enters SMI system interrupt state (Alexander: Column 5 Line 23 – 25); (3) when a SMI is requested, the data is validated first and then unlock the flash memory by issuing a reset pulse to firmware hub (Alexander: Column 5 Line 60 – 62 and Figure 3A / state Element 340 directed to state Element 342) – i.e. this is because to update/flash a valid RBU (after the successful validation) must unlock the flash memory by outputting a reset pulse to firmware hub; and thereby, as a result, (4) the flash memory is reset to a read/write access (i.e. unlock the flash memory) and then update with a new RBU (Alexander: Column 5 Line 30 – 34 / Line 42 – 46) – i.e. there exists a valid RBU image

required to be flashed into the memory, and subsequently, (5) when the update is complete the system moves to power on reset state to perform the power-on self test, reset all blocks in flash memory back to "locked" status again and pass control to run state – similar to the case that there does not exist a new valid RBU required to be flashed (i.e. after the new valid RBU has already been flashed in) into the memory at the computer start-up (Alexander: Column 6 Line 8 – 12). Therefore, the disclosed sequence from (1) – (5) constitutes the complete cycle for the program update in the flash memory. Therefore, contrary to Applicant's assertion, Alexander does teach flashed memory is unlocked and updated after the program is verified that meets the claim limitations (Alexander: Column 5 Line 60 – 62 and Figure 3A / state Element 340 directed to state Element 342).

2. Alexander teaches flashed memory is locked before the program is updated regarding in state 330, the flash memory is reset to a read/write access.

On page 5 (3rd Para), Applicant has alleged that in state 330, the flash memory is reset to a read/write access, as taught by Alexander, is the same as unlocking the flash memory and thereby Applicant asserts Alexander teaches the flashed memory is unlocked before the program is updated as opposed of what is recited in the claim (Appeal Brief, Page 5, 3rd – 4th Para). Applicant further provides Declaration filed on Oct. 24, 2005 (under 37 C.F.R.

§1.132) by Steve Goodman to attest such an assertion. Examiner respectfully disagrees. The purpose of power-on reset state is to access the flash memory in order to get the computer started. In other words, to start a computer, the flash memory is reset to a read/write access, as taught by Alexander, to unlock the flash memory – this is for the purpose of reading the BIOS at start-up which is similar to Applicant's Declaration filed on Oct. 24, 2005 (under 37 C.F.R. §1.132). However, the program update cycle in practice starts from computer runtime mode when the flash memory is locked. As referring to the flash memory update cycle sequence (1) – (5) listed above and the purpose to reset the flash memory into a read/write access (unlocked status), contrary to Applicant's assertion, is indeed to update/flash the valid RBU image into the flash memory after the successful validation of the data (Alexander: Column 5 Line 60 – 62 and Figure 3A / state Element 340 directed to state Element 342) and to update/program the flash memory, the memory block needs to be unlocked and all unlocked blocks return to the locked state again when the device is reset or powered down (Alexander: Column 3 Line 62 – 64: also see above). Therefore, Examiner holds the teaching of Alexander and Grawrock meets the claim limitation recited as "if the signature verification of the update to the program is successful, unlocking a memory unit storing the program; and modifying the program with the update to the program in response to the unlocking of the memory unit storing

the program (Note: refer to the flash memory update cycle sequence (1) – (5) as listed above)".

Note: As per claim 1, 4 and 8, obviousness-type double patenting as being unpatentable over claim 18 (and claim 3) of co-pending Application Serial No. 09/931,550 is maintained upon the resolution with the co-pending application of allowance one way or the other.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Longbit Chai

Conferees:

Gilberto Barron

Matthew Smithers

GILBERTO BARRÓN JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137